National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CGS Port Security Capability

Version 1.1.1

Port Security helps to control access to logical and physical ports, protocols, and services. This includes all Enterprise devices such as network appliances, servers, workstations, and network boundary devices. The Port Security Capability provides the management of logical and physical ports. This Capability also includes an auditing and monitoring function of Enterprise devices to ensure compliance with Port Security policies.

07/30/2012

CGS Port Security Capability
Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Port Security helps to control access to logical and physical ports, protocols, and services. This includes all Enterprise devices such as network appliances, servers, workstations, and network boundary devices.

The Port Security Capability provides the management of logical and physical ports. Port Security management includes deciding which ports, protocols, and services should be available and controlling which services or information may pass to, from, and through the system. This includes making decisions regarding the protection of physical ports and how to lock down services. This Capability also includes an auditing and monitoring function of Enterprise devices to ensure compliance with Port Security policies.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Port Security Capability shall protect a network by controlling which ports are accessible. Maintaining effective Port Security means managing and controlling access to logical and physical ports, protocols, and services on a network. Port Security also includes deciding which ports, protocols, and services shall be available based on understanding data and mission flows and the risk associated with using the port, protocol, or service. The outcome of that decision is passed to Digital Policy Management to establish the policies for ports, protocols, and services use.

The Port Security Capability shall determine which ports and protocols shall be available, and which services shall be allowed to pass to, from, and through the Enterprise, down to the individual system/device level, in accordance with policy and best practices. Port Security principles shall take a layered defense approach at the

network boundary, along the communication path, and at the end-device levels. The Port Security Capability shall leverage information from the Risk Analysis Capability to make those determinations and decide how the System Protection and Network Boundary Protection Capabilities will enforce Port Security. This includes making decisions on protection of physical ports (see Physical Environmental Protections), and how to lock down services. The System Protection and Network Boundary Protection Capabilities shall enforce these rules by allowing only the authorized ports, protocols, and services to be used.

For every device, the purpose and behavior of every open port, from the network boundary to the desktop, shall be identified. Where possible, port usage shall conform to industry standards (e.g., Internet Assigned Numbers Authority [IANA]), which define registered ports and protocols assignment. Unique mission needs or the use of proprietary technologies may necessitate usage of ports that do not conform to industry standards. Port Security shall not allow ports to pass protocols other than those needed by the registered services. Usage of protocols shall be in accordance with the Request for Comments (RFC) for that protocol, which defines message formats and use parameters. Ephemeral ports shall be dynamically opened and closed as needed.

All unused or unnecessary ports, protocols, and services shall be disabled to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Enterprise Monitoring and Intrusion Detection and Prevention Capabilities shall identify and prevent the use of prohibited ports, protocols, and services. The information system shall be configured to provide only essential capabilities and specifically prohibit or restrict the use of unnecessary predefined ports, protocols, and/or services.

There shall be periodic reviews of ports, protocols, and services. When defining ports that need to be opened, the Capability shall take into account the source and destination Internet Protocol (IP) addresses or other identifying information, as well as the type of traffic they need to pass. Timelines shall be defined regarding how long a service or port needs to be operational, and periodic reviews shall be implemented. Unnecessary services residing on devices shall be closed, and those not needing to pass beyond the Enterprise boundary shall be blocked at the boundary. Before any port is opened or closed, tests shall be conducted to verify that it is operationally acceptable to open or close the port. Adding ports, protocols, or services in response to an operational need may require reaccreditation of the system.

Physical devices can be used to control access to logical ports. A network proxy can be used to control access to a particular service if the device is not configurable to deny/allow ports, protocols, and services as required. The decision as to whether to use a physical device is dependent on mission needs of the Organization, and the types of systems required to meet the mission (e.g., if the mission dictates the use of legacy systems, the physical device may need to be used).

The Port Security Capability shall enforce the lock down or disabling of physical ports to ensure that an unauthorized device is not plugged in. The default policies for all ports shall be set to deny. When functional needs of the network necessitate ports being opened, each port shall be explicitly allowed on an individual basis following a risk analysis and determination that the need is justified. If the device cannot be configured to deny/allow, mechanisms shall be provided to enable ports to recognize a connecting device to ensure that only authorized devices can connect. This Capability works with the Physical and Environmental Protections Capability to prevent unauthorized devices from connecting to physical ports.

The Configuration Management Capability validates ports, ensures ports are configured as expected, detects changes, and ensures compliance. All port usage changes shall be logged via the Enterprise Audit Management Capability, and monitoring provisions shall be in place, including Host and Network Intrusion Detection Capabilities. Regular audits are conducted to ensure that all policies and procedures are being followed properly and to reevaluate the need for each open port to ensure that a functional need still exists.

Auditing of both physical and logical ports shall occur to ensure that for physical ports only known functions and services are turned on and for logical ports only known ports are enabled. This Capability shall leverage the Enterprise Audit Management Capability for the logging of usage and changes and correlation with other events.

4   Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.
1. Digital policy management exists to establish the digital policies for which ports, protocols, and services shall be used.

2. Configuration management exists to validate and ensure that ports are configured as expected and detects a change.
3. Audit management exists to correlate logs if port, protocol, and service usage changes.

5   Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. This Capability manages both logical and physical ports.
2. This Capability allows physical devices to be used to control access to logical ports.

6   Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

A properly implemented Port Security Capability will fulfill its role in protecting a network by controlling which ports are accessible. Each Organizational policy will provide the management and control of access to ports, protocols, and services.

Organization policy will by default deny access to all ports. Where there is a justifiable functional need for port to be opened, the Organization will have processes in place to individually vet the need to ensure the risk of opening the port is justified. The Organization will maintain records of all open ports and the reasons for that decision. Where possible, those ports that are allowed will follow established protocol standards in place (e.g., Hypertext Transfer Protocol [HTTP] 80/Transmission Control Protocol [TCP], Secure Shell [SSH] 22/TCP, Domain Name Service [DNS] 53/User Datagram Protocol [UDP]) and comply with IANA standards and the Organization's appropriate Ports, Protocols, and Services Management program (see Directives and Policies table for additional details).

The Organization will apply these port management rules to all ports. This includes ports used for internal Enterprise connections and for connections being made with

enclaves external to the Enterprise. For external connections, the Organization will manage port usage for inbound and outbound connections. Inbound and outbound connections to the Enterprise will be separately filtered through the appropriate Network Boundary Protection mechanisms. This will prevent intentional or unintentional connections to unauthorized ports or services originating from inside a network. Each Organization will ensure the following:

- Default setting on all routers and firewalls will be set to Deny All, Permit by Exception (DAPE).
- Dynamic ports will be assigned as needed.
- Port restriction will take place internally and at network boundaries.

The Organization will turn off ports, as directed by Organizational policy, when the protocol is not secure. There may be some exceptions to this from time to time, but allowing the use of protocols that are not secure is highly discouraged. Exceptions are authorized only when the mission need is sufficient to offset the operational risk produced by enabling the use of an insecure protocol. An example of an acceptable use might be a File Transfer Protocol (FTP) server strictly used for documents intended for public consumption, such as press releases.

For every device, each Organization will identify the purpose and behavior of every open port, from the network boundary to the desktop. When defining ports that need to be opened, Organizations will take into consideration the source and destination IP addresses (or other identifying information), including the type of traffic they need to pass, and will define how long a service or port needs to be operational. Prior to opening or closing a port, the Organization will perform testing to ensure there is no negative operational impact. Organizations will use the Configuration Management Capability to enforce port usage rules dictated by Digital Policy Management. Where exceptions must be made, the Organization will ensure they are well documented and limited in scope as much as possible.

Because risk and functional need changes over time, the Organization will provide periodic reviews to reassess any open ports and verify that the operational need still exists and still justifies the risk. Services that may reside on devices that are not needed will be closed, and those that are not needed to pass beyond the Enterprise boundary will be blocked at the boundary. When new ports are opened or timelines are extended, the Organization will specify a time period for the review of the rule.

The Organization will ensure various other Community Gold Standard Capabilities are in place for proper port management. The Organization will leverage the Enterprise Audit Management Capability to perform regularly scheduled audits to verify that all security measures are in place and effective. Network Boundary Protection is used to control traffic coming into a network and ensure that packets destined for blocked ports are dropped. The Organization will use Intrusion Detection to locate any unauthorized port usage by scanning traffic that does come through to ensure that it is both safe and not in some way circumventing the port controls. In addition, procedures will be in place for Host Intrusion Detection to ensure only authorized ports are in use.

Organizations will also use security mechanisms such as port protection devices, as needed. Fitted to a communications port of a host computer, a port protection device authorizes access to the port itself, often based on separate authentication (such as a dial-back modem) mechanisms independent of the computer's own access control functions. Organizations will use port protection devices when a device has a port that is not configurable.

Securing logical ports alone is not enough. Organizations will put measures in place that prevent intruders from being able to enter a facility and connect to physical ports (see Physical and Environmental Protections Capability for additional details). Some of these measures include protections such as facility entrance and other technical protections for physical ports. Each Organization will ensure auditing of both physical and logical ports shall occur and leverage the Enterprise Audit Management Capability for the logging of usage and changes and correlation with other events.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Network Mapping Capability provides the visibility necessary to determine what needs to be protected and where. The Port Security

Capability must understand what network components are in the Enterprise to appropriately control the ports, protocols, and services active on the network.

- Network Boundary and Interfaces–The Port Security Capability relies on the Network Boundary and Interfaces Capability for information about ports, protocols, and services that are used internally and externally for Enterprise boundaries and interfaces.
- Understand Mission Flows–The Port Security Capability relies on the Understand Mission Flows Capability for information about mission flows, which provides insight into understanding what ports, protocols, and services need to be allowed.
- Understand Data Flows–The Port Security Capability relies on the Understand Data Flows Capability for information about data flows, which provides insight into understanding what ports, protocols, and services need to be allowed.
- System Protection–The Port Security Capability relies on the System Protection Capability to enforce security settings established by the Port Security Capability at the system level.
- Communication Protection–The Port Security Capability relies on the Communication Protection Capability to secure transmissions using authorized logical ports on the network.
- Physical and Environmental Protections–The Port Security Capability relies on the Physical and Environmental Protections Capability to employ protection mechanisms to control access to physical ports.
- Configuration Management–The Port Security Capability relies on the Configuration Management Capability to ensure that only authorized ports are used on the network.
- Network Boundary Protection–The Port Security Capability relies on the Network Boundary Protection Capability to ensure that only authorized ports, protocols, and services pass across network boundaries.
- Digital Policy Management–The Port Security Capability relies on the Digital Policy Management Capability to establish the digital policies that determine which ports, protocols, and services should be used by each system or device.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Port Security Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.

- IA Policies, Procedures, and Standards–The Port Security Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Port Security Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Port Security Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Port Security Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3   Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Enterprise Monitoring–The Port Security Capability relies on the Network Enterprise Monitoring Capability to provide information used to identify and prevent the use of prohibited ports, protocols, and services.
- Network Intrusion Detection–The Port Security Capability relies on the Network Intrusion Detection Capability to provide information used to identify and prevent the use of prohibited ports, protocols, and services.
- Host Intrusion Detection–The Port Security Capability relies on the Host Intrusion Detection Capability to detect any unauthorized port usage on host systems.
- Network Intrusion Prevention–The Port Security Capability relies on the Network Intrusion Prevention Capability for information to identify and prevent the use of prohibited ports, protocols, and services.
- Host Intrusion Prevention–The Port Security Capability relies on the Host Intrusion Prevention Capability to identify and prevent the use of prohibited ports, protocols, and services on host systems.
- Risk Mitigation–The Port Security Capability relies on the Risk Mitigation Capability to determine which ports, protocols, and services can be used and under what conditions.

8   Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-7 *LEAST FUNCTIONALITY*	Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]. Enhancement/s: (1) The organization reviews the information system [Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services. (3) The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].

9   Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Port Security Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National

National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), 13 August 2004, Unclassified	Summary: This instruction implements policy on using ports, protocols, and services in Department of Defense (DoD) information systems in a manner that supports the evolution to net-centric operations.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction provides joint policy and guidance for information assurance (IA) and Computer Network Defense (CND) operations. The policy covers ports, protocols, and services (PPS) intended for use in DoD information systems or that traverse between DoD enclaves. It specifies that they will undergo a vulnerability assessment; be assigned to an assurance category; be registered; be regulated based on their threat potential to cause damage to DoD operations and interests; and be limited to only PPS required to conduct official business in accordance with (IAW) DoD Instruction (DoDI) 8551.1.
DISA Network Infrastructure Security Technical Implementation Guide (STIG), version 7.1, 25 October 2007, Unclassified	Summary: This Security Technical Implementation Guide (STIG) provides security considerations at the network level needed to achieve an acceptable level of risk for information as it is transmitted through an enclave. It was developed to enhance the confidentiality, integrity, and availability of sensitive DoD automated information systems.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	

Legislative	
Nothing found	

Port Security Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Internet Assigned Numbers Authority (IANA), Unclassified	Summary: This document allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. It is responsible for maintaining many of the codes and numbers contained in a variety of Internet protocols.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Scope of work–The Enterprise needs to consider the amount of traffic crossing network boundaries and the number of ports this Capability is responsible for managing. The larger and more complex these factors, the greater the total cost will become.
2. Network bandwidth availability and consumption–This Capability must maintain system and service availability requirements despite the overhead required to fulfill its functions.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Port Security Capability.

- The Enterprise shall provide for the management of logical and physical ports, protocols, and services including the management of which ports, protocols, and services should be available and controlling which services or information may pass to, from, and through the system. The Enterprise shall make decisions regarding the protection of physical ports and how to lock down services,

including auditing and monitoring of Enterprise devices to ensure compliance with port security policies.

- The Enterprise shall manage and control access to logical ports on the network.
- The Enterprise shall manage and control access to physical ports on the network.
- The Enterprise shall manage and control protocols in use on the network.
- The Enterprise shall manage and control services in use on the network.
- The Enterprise shall determine which ports, protocols, and services to allow based on understanding data and mission flows and the risk associated with use of each port, protocol, or service.
- For every device, the purpose and behavior of every open port, from the network boundary to the desktop, shall be identified.
- The Enterprise shall ensure that all ports used by the network conform to industry standards.
- The Enterprise shall ensure that all ports pass only protocols that are needed by registered services.
- Usage of protocols shall be in accordance with the Request for Comments for that protocol, which defines message formats and use parameters.
- Ephemeral ports shall be dynamically opened and closed as needed.
- All unused or unnecessary ports, protocols, and services shall be disabled or blocked to prevent unauthorized activity.
- Systems shall be configured to provide only essential capabilities and specifically prohibit or restrict the use of unnecessary predefined ports, protocols, and services.
- All approved ports, protocols, and services shall be periodically reviewed to assess whether they are still necessary to mission operations.
- When allowing a port, protocol, or service to be used on the network, the Enterprise shall document the mission need and other relevant information as specified by Organizational policy.
- Before any port is opened or closed, tests shall be conducted to verify that to open or close the port is operationally acceptable.
- Systems shall be reaccredited, as necessary, based on configuration changes from allowing new ports, protocols, or services.
- The Enterprise shall ensure that all physical ports are only enabled for network connectivity when an authorized device is connected.
- The Enterprise shall ensure that all systems are configured properly in accordance with approved port usage policies.

- Changes to port activity shall be logged as auditable events and audited in accordance with Organizational policy.